Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2015

Date filed: 1 March 2018

Name of company covered by this certification: Precision Communications, Inc. (dba PCI Broadband)

Form 499 File ID: 827607

Name of signatory: David Wainwright

Title of signatory: Vice President

I, David Wainwright certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how PCI Broadband's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

PCI Broadband has not taken any actions, instituted court proceedings, or filed any petitions at either state commissions, the court system, or at the Commission against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI data. In addition there have been no instances of unauthorized disclosure of CPNI data to a individual not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

Signed David J Wainwright [electronic signature]
Vice President

Attachment 1

PCI Broadband is pleased to submit the following statement which shows how the PCI Broadband CPNI data protection procedure is in compliance with section 64.2001 et seq. of the Commission's rules.

The PCI Broadband CPNI data protection procedure uses account authentication to insure that call detail information is not released during a customer-initiated telephone contact.

All PCI Broadband customers have established a personal password with PCI Broadband. All employees know how to verify the customer established password. If the customer does not confirm the pre-established password then employees know that no private personal information, billing information, or call detail can be given out over the phone.

The PCI Broadband CPNI data protection procedure does allow for the mailing of the information to the customers address of record if the customer requests such mailing to take place.

In an extreme case PCI Broadband employees could also call the customer's telephone number of record and disclose information.

PCI Broadband's procedures also cover online account access. All PCI Broadband customer portal web sites have password protection before a customer could see any billing information, change a password or see call detail records.

At the main PCI Broadband office PCI Employees may provide account information to customers who present a valid photo ID.

PCI Broadband has initiated a procedure to notify customers immediately of a change of password to an online account or customer's address of record. PCI Broadband's electronic system takes note of the event of a change and writes it to PCI Broadband employee action page. PCI Broadband employees take note of the account change and will either call the customer telephone number of record and leave a voice mail or send a letter about the account change through the US Postal System. PCI Broadband's procedure does not allow the employee to disclose what account information was changed.

PCI Broadband's procedures address what to do in the event of a breach of CPNI data. First the employee will bring the breach information to their immediate supervisor. The immediate supervisor will bring the information to the PCI Broadband CPNI data protection custodian. The data protection custodian will make an electronic notification to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") immediately and in no instance longer than seven business days from the date of breach.

The PCI Broadband procedure calls for the PCI Broadband CPNI data protection custodian to notify affected customers after seven business days have elapsed after electronic notification of the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI").

The PCI Broadband CPNI data protection custodian must make a determination if the data breach could cause immediate and irreparable harm to the affected customers. If the PCI Broadband CPNI data protection custodian's determines waiting seven business days will cause immediate and irreparable harm to the customers he will include this determination in the electronic notification and than consult with the investigating agency before notifying the affected customers. In all cases the PCI Broadband CPNI data protection custodian will consult with the investigating agency and abide by all agency directives in the release of information of the breach to the affected customers.

The PCI Broadband CPNI data protection custodian is required to maintain customer CPNI data breach information for a minimum of two years.

The PCI Broadband CPNI protection procedure only allows for customer opt-in consent before any customer CPNI information is released to a PCI Broadband joint venture partner or independent contractor. The customer must opt-in by returning a signed PCI Broadband form authorizing the disclosure of CPNI information to a PCI Broadband joint venture partner or independent contractor.

The PCI Broadband CPNI protection and disclosure procedure document is maintained at the company's main office at 6285 Lehman Dr. Suite 100, Colorado Springs, CO, 80918 and is available for public review at that location. The PCI Broadband CPNI protection and disclosure document is part of PCI Broadband's employee training and all current PCI Broadband employees must pass a written test on the Procedure before working with the public.